Supporting Resource 2d

GUIDE and TEMPLATE for developing a GBV Administrative data Information Sharing Protocol (ISP)

This document includes GUIDANCE and a TEMPLATE for developing an Information Sharing Protocol (ISP) to regulate the sharing of administrative data collected about gender-based violence in the context of GBV service provision.

This document is adapted from the GBVIMS 2014 template and guidance. This document is prepared for organizations/agencies sharing GBV administrative data but not using the GBVIMS. For more information about the GBVIMS, visit www.gbvims.org

NOTE: The term 'Survivor' is used throughout this document to represent victim/survivors. Consideration should be given to the terminology if homicide victims are included in the database.

Gender-based Violence Administrative Data Information Sharing Protocol Guidance

Contents

Introduction to Information Sharing Protocols

In any context where information or data is shared between agencies, Information Sharing Protocols (ISPs) are an important tool to ensure safe, ethical and transparent processes. This is particularly true when sharing sensitive and confidential information such as gender-based violence (GBV) administrative data.

GBV administrative data and information is highly sensitive, and the risks and potential benefits of sharing this information must be carefully considered. While producing regional, inter-agency or service level statistics on GBV is important, service providers must prioritise clients' rights to confidentiality and privacy, and ensure all information sharing practices are safe.

When sharing GBV data, it is important to avoid common mistakes:

- Only share survivors' data or information with their knowledge and consent
- Understand how data will be used, and what level of data will be shared
- Ensure the safety and security of survivors and service providers
- Reciprocate information sharing
- Documented processes or procedures to regulate information sharing

Good practice around information sharing is essential to enable inter-agency coordination and collaboration, ensure the use of GBV administrative data is as effective and safe as possible, and support informed service provision. This in turn supports the safe, ethical, and transparent use of GBV administrative data to illustrate trends in service use, highlight gaps and opportunities for improvement, and strengthen advocacy and programming to end gendered violence. Unless agencies intending to share information have established common understanding, and documented their expectations and processes, lack of consensus and discrepancies can arise very quickly.

Information Sharing Protocols aim to help address some of these challenges by setting out clear guidelines, expectations, and processes for sharing GBV data and information. Developing an Information Sharing Protocol around GBV administrative data sharing will:

- Open discussions that promote ethical, safe data sharing, and ensure the potential risks and benefits of doing so are considered.
- Establish a clear, shared understanding of what information will be shared, the purpose of sharing this information, when information will be shared, by whom and how.
- Define the roles and responsibilities of each agency or partner sharing information.
- Establish how the data will be used, including if and how agencies will be credited or protected in the publication of any statistics.

Strong relationships in the Pacific region

Strong personal and community relationships often underpin service delivery in the Pacific, with individual workers and leaders driving key initiatives and processes like information sharing. This way of working is extremely positive in that it is based on trust and grounded in local communities; however, it is vulnerable to disruption and may not be sustainable if key people leave or become unavailable. Developing and implementing an ISP can help to embed practices into organisations and services, guarding against these vulnerabilities. An ISP does not replace strong relationships based on trust but helps to guide processes and ensure that strong relationships and practices can be maintained over time.

Agencies involved in data sharing may take on one or more of the following roles, depending on the purpose of information sharing and the agreed structures and systems in place.

- Data gathering agency: Gathers data according to agency protocols, and shares data specified in the ISP with the agency responsible for consolidating the information.
- Consolidating agency: Receives information from data gathering agencies, and consolidates/compiles it, and reshares the information according to the specific ISP agreements.

Developing an effective Information Sharing Protocol

How you approach the development of an ISP is just as important as the final document. For the ISP to be as effective and sustainable as possible, the development process needs to be participatory, collaborative, inclusive and respectful of all partners involved. Without a robust process that is inclusive of all partners, trust will not be well developed, and implementation of the final ISP may be hindered.

The process to develop and implement an ISP involves the following broad phases:

- Collect data and identify information sharing needs
- Identify information sharing partners and key contacts
- Clarify the structure, outcomes and formats of information to be shared
- Agree on reporting, timelines, use and constraints for the ISP
- Develop a dissemination and implementation strategy

Agencies looking to develop an ISP around GBV administrative data can use the following steps and key questions to guide the process.

Key sections of an ISP

Purpose	The intent behind the protocol, and the reasons for GBV administrative data and information sharing.
Ground rules	Basic rules and expectations for signatories sharing information. It defines the responsibilities of implementing agencies, and responsibilities of any national or regional/sub-national agencies involved in information consolidation.
Data security	Precautions and considerations for ensuring that the security of all data and of the participating agencies collecting data are maintained.
Consolidating agency	The role of the consolidating agency (if applicable), including its relationship to data gathering agencies.
Internal information sharing procedures and reports	What information will be shared, the frequency this will be done, and the areas to be included in reports submitted to the consolidating agency.
When others request GBV information	Procedures to follow when external agencies or other actors (e.g., media, government, agencies not included in the ISP), request GBV information
Time limit	The duration for the ISP, and a date for review and renewal of the ISP.
Breaches	What constitutes a breach of the protocol, and steps to be taken if a breach occurs.
Annexes	Examples (based on templates or ‘dummy’ data) of how information should be formatted. Includes a list of agency contact and focal points, and the data protection protocol.

STEPS AND KEY QUESTIONS FOR DEVELOPING AN ISP

Steps	Description	Key questions to ask
Step 1	Decide whether an ISP is appropriate for your context.	• Does the agency regularly share GBV administrative data, or is it looking to do this? • Are there any protocols already in place?
Step 2	Consider who you will be sharing data with and reach out to open a discussion with them.	• Which service providers do we already share information with? • Who do we not share information with? • Who do we need to share information with?
Step 3	Establish and agree on what level of information sharing is most appropriate for your context.	• What level of information is useful for the agency? • What level of information is useful to partner agencies? • What level of information is safe to share? • Are these levels of information possible to share?
Step 4	Identify and articulate the purpose and expected outcomes of sharing information. Decide *what* information needs to be shared.	• What is the purpose of sharing information with this partner agency? • What do we expect the outcomes will be if we share information? • What information will we be sharing?
Step 5	Draft the 'purpose' section of your ISP, making sure to include expected outcomes of sharing information.	• Is the purpose of sharing information clearly articulated? • Are expected outcomes of information sharing expressed clearly?
Step 6	Establish what the flow of information will look like, and *how* the information will be shared.	• Is information to be shared both ways between agencies? • Will information be shared in hard copy or digitally? • What capability do we have to share information digitally? • If sharing hardcopy data, what logistics need to be considered?
Step 7	Establish what the roles and responsibilities of all agencies involved will be.	• Who is involved and what are their roles? • Who will be responsible for which aspects of the ISP? • Who will be responsible for compiling shared data?
Step 8	Decide on the format of reporting and how often/when this will happen. Include an expiration date and date of review for the ISP. Set a date to reconvene with partners to reassess.	• What format will reports be produced in? • How often will reports be produced? • What is the expiration date of the ISP? • When will partners convene to discuss changes or reviews?
Step 9	Agree on how information will be used, and not used. This includes how submitted and compiled data will be stored, analysed and utilized.	• Where will data be stored? • How will the data be analysed, and by whom? • How will data be used, and what is the scope of this use? • How will data *not* be used? • What constitutes a breach of how information can be used?
Step 10	Ensure privacy and confidentiality measures have been considered throughout previous steps.	• Are the privacy and confidentiality of clients, practitioners, and agencies ensured? • Are there any gaps or risks for any of the above?

Step 11	Determine the consequences for a breach of the ISP will be.	• What constitutes a breach of this ISP? • How will a breach of the ISP be handled and by whom? • What will the consequences of a breach be?
Step 12	Use the information from steps 1 through 11 to draft the full ISP.	• Does the ISP draft address the key questions? • Have all partners reviewed the draft and provided feedback/input? • Who will finalise and sign off on the ISP? • Have all partners signed the finalised ISP?
Step 13	Ensure the finalized, signed ISP is shared with all signatories and at all relevant GBV working group meetings.	• Do all signatories have a finalized copy of the ISP? • Has the ISP been shared with all appropriate partners?
Step 14	All signatories notify staff of the ISP, including the development process and any additional guidelines.	• Have all signatories/agencies notified their staff of the ISP? • Is there a process in place to effectively implement the ISP? • Are there other guidelines needed to support the ISP?

STEPS AND KEY QUESTIONS FOR IMPLEMENTING AN ISP

Steps	Description	Key questions to ask yourself
Step 1	Begin collecting and sharing data as set out in the ISP.	• Have all partners begun implementing any changes to the way they collect data? • Is the process of sharing data up and running as expected? • Is the consolidating agency receiving information from data gathering agencies as expected?
Step 2	Compile collected data.	• Is data compiled effectively? • Has data been effectively de-identified in the compilation process?
Step 3	Share compiled information back to data gathering agencies (if applicable).	• Is compiled information being shared back to agencies appropriately and in the expected format? • Is the data held and transferred securely and confidentially? • Have any gaps emerged, or any unexpected risks been identified?
Step 4	Explore shared data and how it can inform coordination and collaboration.	• What picture is emerging from the data, as a whole and for each agency? • Are gaps being identified in the compiled data that can be addressed or used to improve services? • How does the shared data inform service collaboration?
Step 5	Based on Steps 1 – 4, review the ISP and address any changes that might be needed.	• Who will be involved in reviewing the ISP and who will lead the process? • What is the timeframe for review and amendment? • How will amendments be communicated and taken forward into practice?

Next steps for implementation

Once an ISP has been developed, implementation becomes the primary focus. Note that because GBV administrative data is collected continuously, implementation of an ISP in this area will require cycles of development, testing, review, and amendment to ensure it remains relevant and effective. The following phases of action can be taken following the initial development of an ISP:

- Compile data and produce agreed outputs
- Share data back to data gathering organisations
- Analyse data for coordination
- Use data to improve services and inform policy
- Review the ISP and implementation of any changes needed

TEMPLATE for developing a GBV Administrative Data Information Sharing Protocol (ISP)

Information you will need to change to reflect your organisation/context is highlighted in yellow. You may delete this text box and logos as needed to prepare your Information Sharing Protocol.

NOTE: This is a generic template based on the GBVIMS. Any organization using this template to draft an ISP should have their final document reviewed by their legal team to ensure local legal requirements are met along with any international requirements.

GBV Administrative Data

Information Sharing Protocol between data gathering organizations:

[LIST DATA GATHERING ORGANIZATIONS] (DGOs) and [CONSOLIDATING AGENCY]

In [GEOGRAPHIC REGION COVERED BY ISP]

PURPOSE

This information sharing protocol is to set out the guiding principles and describe procedures for sharing anonymous data on reported cases of GBV captured by the [FULL NAME OF AGREED UPON CONSOLIDATING AGENCY] ([CONSOLIDATING AGENCY'S ACRONYM]) in its capacity as [CONSOLIDATING AGENCY'S ROLE] for GBV prevention and response work in [OPERATIONAL / GEOGRAPHIC REGION] in [NAME OF COUNTRY]. The protocol is meant to facilitate information sharing between participating actors.

The signatories to this agreement recognize that sharing and receiving non-identifiable GBV data will contribute towards improved inter-agency coordination, identifying and targeting gaps, prioritization of actions, and improved programming of prevention and response efforts. It may also result in improved advocacy efforts, increased leverage for fund raising and resource mobilization, and improved monitoring. All agencies will protect information to ensure that no harm comes to any survivor, service provider or the community from information sharing efforts.

GROUND RULES

- Information submitted by data gathering organizations to **[CONSOLIDATING AGENCY]** will be submitted in the agreed-upon format and **will not contain any identifying information of survivors or agencies**. Non-identifiable GBV data is context specific but excludes data points that could result in a survivor (or, in some cases, those organizations providing services to them) becoming known outside of the context of the care survivors are receiving. In some contexts, data such as exact age together with the incident location can reveal a survivor's identity. The data points to be shared must consider all possible outcomes that could lead to a survivor being identified and must consider both the number of cases being reported and the context.
- The information shared by data gathering organizations will be consolidated by **[CONSOLIDATING AGENCY]** into a monthly aggregate report. This report will be shared back to the data gathering organizations for further shared analysis.
- All signatories agree that the **GBV data will not be used for following up on individual cases**.
- All agencies will protect information to ensure that no harm comes to any survivor, service provider or the community from information sharing efforts.
- Information sharing should only happen with the **informed and free consent of GBV survivors**, and all interaction with survivors should follow a survivor-centered approach.
- Each data gathering organization reserves the right to share its own data externally, for example for internal and donor reporting requirements, resource mobilization, and advocacy. Even when using its own data externally, each GBV data partner is expected to do this in a responsible manner that **maintains the safety and security of GBV survivors, service providers and their communities**. Each data gathering organization may suspend the sharing of information for reasons of safety, security, capacity or other considerations through written justification to other ISP signatories.
- New partners who are offering health and/or psychosocial services to GBV survivors will be added to the protocol once they have met the following criteria:
    1. They have received the appropriate training and follow-up support to implement the GBV data collection within their own operations and have demonstrated good comprehension of the safety and risks to survivors.
    2. They have reviewed the ISP and discussed the process for information sharing within the **[GBV administrative data Working Group/Task Force]**.
    3. They have organizational support for data sharing.
    4. Signatories to this ISP have been consulted regarding inclusion of new partners to this agreement.
- For security purposes and to ensure survivor confidentiality, **no survivor-specific information that can lead to identification of the survivor will be shared**, e.g., name, initials, address, phone number, etc. All information shared will be anonymous statistical data.
- Following signature of the protocol, the data gathering organizations' and consolidating agency's focal points have a **responsibility to train their colleagues** about the standards and procedures outlined in this information sharing protocol. Notably, that GBV administrative data is shared on a **[FREQUENCY]** basis among ISP signatories in the manner outlined in this document; any requests from external actors for access to consolidated GBV information must be directed to the **[CONSOLIDATING AGENCY]** focal points in order to begin the authorization process among the data gathering organizations; GBV administrative data is not to be used for following up or investigation on individual cases/survivors. They should also explain to their colleagues that any question or request for GBV information should be directed to their respective organizations' GBV data focal points.

- GBV administrative data is shared on a **[monthly]** basis among ISP signatories in the manner outlined in this document. Any requests from external actors[1] for access to GBV data has to follow the procedure outlined below.

DATA SECURITY

[CONSOLIDATING AGENCY] and the data gathering organizations will ensure that all data is safe and secure and will implement appropriate procedures to maintain confidentiality of the data. Organizations will submit an Excel document and will employ password protection. The ***password for these submitted files*** has been agreed upon by each data gathering organization and shared with **[CONSOLIDATING AGENCY]**.

[CONSOLIDATING AGENCY] has outlined during the creation of this protocol how the data will be:

- Received: Email to **[CONSOLIDATING AGENCY]** GBV data Focal Points[2]
- Stored/deleted: See Annex **XX** Data Protection Protocol
- Protected in the computer: See Annex **XX** Data Protection Protocol
- Used by whom (who has access to the data and the computer) GBV data Focal Points

The **[FREQUENCY]** reports in **[TYPE OF DATA TO BE SHARED]** form are shared with the **[CONSOLIDATING AGENCY]** GBV data Focal Points/Liaison, in the organization's capacity as **[CONSOLIDATING AGENCY'S ROLE]**. In case the security situation deteriorates in **[GEOGRAPHIC REGION COVERED BY ISP]**, hampering **[CONSOLIDATING AGENCY]**'s or the data gathering organizations' abilities to protect and assist survivors or their information, the information sharing protocol will be reviewed and consequently adapted to respond to the changing environment. The **[GBV administrative data Partners/Taskforce]** will develop contingency plans for data security and information sharing should the security situation change.

[FREQUENCY OF REPORT] REPORT

[FREQUENCY OF REPORT] Report

1. Frequency: Data gathering organizations (DGOs) will submit **[type of data]** (defined in Annex **XX**) for all new cases reported during the previous period to **[CONSOLIDATING AGENCY]** by the **[AGREED UPON DAY OF SUBMISSION]** of each **[FREQUENCY]** in a password protected document. For the purpose of compilation and data sharing, this is the only reporting format that will be requested of DGOs.
2. Areas of coverage: The aggregate reports will reflect the following geographical areas based on the data gathering organizations providing data. **[TABLE/LIST GEOGRAPHIC AREAS AND ASSOCIATED DATA GATHERING ORGANIZATIONS]**
3. **[CONSOLIDATING AGENCY]** will consolidate all submitted data and create an aggregate **[FREQUENCY]** report (see Annex **XX**) with all data gathering organizations' identifying information removed. This will be sent back to all the data gathering organizations by the **[AGREED UPON DAY OF SUBMISSION]** of each **[FREQUENCY]** after removing all data gathering organizations' identifying information. This **[FREQUENCY]** report will be shared back to all data gathering organizations with a summary of key

[1] For the purpose of this ISP, "external" refers to any entity that is not a signatory to the ISP.

[2] See the Focal Point document.

findings by **[CONSOLIDATING AGENCY]** within **[AGREED UPON TURN-AROUND TIME]** of the **[FREQUENCY]** data analysis meeting.

4. The GBV Administrative Data ISP signatories will meet once a **[FREQUENCY]** to discuss trends and patterns in reporting. **[CONSOLIDATING AGENCY]** will compile the analysis during this meeting to include in a **[FREQUENCY]** report on GBV trends in **[AGREED UPON GEOGRAPHIC AREA]**. The format of this report will be agreed upon by the actors during this **[FREQUENCY]** meeting, but it should not include consolidated figures (i.e. numbers). The aim of the **[FREQUENCY]** report is to provide a snapshot of GBV reporting in **[AGREED UPON GEOGRAPHIC AREA]** to inform responses and advocacy across non-GBV data contributing agencies and for external uses as necessary (e.g Sectoral meetings).

Agency Focal Points: The individuals responsible for the submission of data and for sending compiled **[FREQUENCY]** reports are listed in the GBV administrative data Focal Point document (**Annex XX Focal Points Document**). Each organization or agency that is part of the GBV administrative data Task Force should have a primary and second GBV data Focal Point to fulfill the roles and responsibilities (**See Annex XX Roles and Responsibilities**) related to the roll out of the GBV data system. In the case of staff turnover, each agency is responsible for designating a new focal point, doing a complete handover of GBV data responsibilities, and communicating this change to the **[CONSOLIDATING AGENCY]** GBV data Focal Point/Liaison, who will be responsible for updating the GBV administrative data Focal Point document. In case no update is provided about the new GBV data Focal Point, **[CONSOLIDATING AGENCY]** GBV data Focal Point/Liaison will contact the senior management of the concerned agency to obtain the new focal point details, and update **Annex XX Focal Points Document**.

[Name Frequency of Report (if there are additional) to include points listed above]

WHEN OTHERS REQUEST GBV INFORMATION

Internal and Donor Reporting

[CONSOLIDATING AGENCY] and GBV data gathering organizations are authorized to use consolidated statistics on reported GBV incidents for their internal and donor reporting requirements.

When sharing data for their internal reporting requirements, organizations and agencies should maintain data protection standards of confidentiality and security. In that purpose they should send the following caveat along with the GBV statistics:

> *The data shared is only from reported cases, and is in no way representative of the total incidence or prevalence of Gender-Based violence (GBV) in **[AREA OF COVERAGE]**. These statistical trends are generated exclusively by GBV service providers who have signed the GBV Administrative Data ISP for data collection in the implementation of GBV response activities in a limited number of locations across **[AREA OF COVERAGE]**and with the consent of survivors. This data should not be used for direct follow-up with survivors or organizations for additional case follow-up. The following information should not be shared outside your organization/agency. Failure to comply with the above will result in the suspension of sharing GBV data and statistics in the future.*

[CONSOLIDATING AGENCY] and GBV DGOs can share information with each other without seeking approval from all the signatories. Additionally, individual DGOs may authorize external sharing of its information bilaterally with another DGO.

It is not recommended to include the media as a pre-approved point for information sharing as context and security situations can change rapidly. Media requests should be handled on a case-by-case basis and in a transparent manner.

Pre-Approved Information Sharing to Non-ISP Signatories [if applicable, for example sharing with other government departments by request]

The agencies/entities below have been approved by all ISP signatories to access the agreed-upon consolidated data reports for the specific purposes mentioned.

Who	Location	Purpose	Format

Every [FREQUENCY], [CONSOLIDATING AGENCY] GBV data Focal Point/Liaison will prepare and share the agreed tables and/ or summary of trends (**Annex XX: Data Set to be Shared with Pre-Approved Non-ISP Signatories**) including the caveat above with the following pre-approved external actors, who have been agreed upon by all signatories to this ISP.

The standard consolidated data reports to be shared with pre-approved external actors will be shared by [CONSOLIDATING AGENCY] with all signatories XX days before sending the reports. These XX days will provide the signatories with an opportunity to review the reports and raise any potential errors and/or concerns.

If any of the pre-approved partners request information which is outside of the pre-approved format or purpose, they should also submit a request according to the criteria listed in the following section.

Other External Actors

Each time external agencies or actors not already approved for data sharing by the ISP signatories submit a request for any other consolidated GBV administrative data, [CONSOLIDATING AGENCY] GBV data Focal Points/Liaison will issue a written request to each of the data gathering organizations for authorization to share aggregate consolidated data. Each request for authorization to share consolidated GBV data will specify:

- The reason/purpose for the request for information,
- What the information will be used for
- How the information will be used,
- How the information produced with the consolidated data and analysis will be fed back to the data gathering organizations, and
- A written guarantee by the receiving party to not disseminate the report to any other party or utilize it for any purpose beyond that which was requested and authorized.

The consolidated data will be shared only after receiving authorization from one of the identified focal points from each of the data gathering organizations.

If signatories to the ISP (other than [CONSOLIDATING AGENCY] GBV data Focal Points/Liaison) receive requests from external agencies or actors not already approved for data sharing by the signatories, they should inform and send this request to [CONSOLIDATING AGENCY] GBV data Focal Points/Liaison so that the appropriate action is taken.

When a request for authorization to share data is submitted by [CONSOLIDATING AGENCY]:

1. The request will be sent by [CONSOLIDATING AGENCY] GBV data Focal Point/Liaison to both the primary and secondary focal points of each organization.
2. [CONSOLIDATING AGENCY] GBV data Focal Point/Liaison will call the focal points of each organization to inform them about the request received, and ask them to provide their written feedback to the request within **5 business days**. [CONSOLIDATING AGENCY] GBV Focal Point/Liaison will also follow up with the organizations' focal points by telephone.
3. If no response is received from the organizations' focal points, [CONSOLIDATING AGENCY] GBV data Focal Point/Liaison will follow up with the senior management of the non-responsive organization(s). If no response is received from the senior management after 5 business days, it does not imply automatic authorization to share the data externally.
4. If after following the above steps, the organization(s) has/have still failed to provide feedback, [CONSOLIDATING AGENCY] GBV data Focal Point/Liaison will contact those organizations who have already provided their authorization and ask them whether they agree to share the aggregated data excluding the data collected by one (or more) signatories that is/are not responding to the request.
5. If all organizations still agree to data sharing, then data will be shared excluding the data collected/compiled by the non-responsive organization(s).

[CONSOLIDATING AGENCY] GBV data Focal Point/Liaison will remove all data gathering organizations' identifying information.

A party that has been authorized to receive consolidated GBV data must agree to not disseminate the information to any other sources in the written request they submit to [CONSOLIDATING AGENCY] GBV data Focal Point/Liaison. The party has to direct any requests they receive for access to this shared data to [CONSOLIDATING AGENCY] GBV data Focal Point/Liaison.

When written authorization for external data sharing is attained from GBV data gathering agencies, [CONSOLIDATING AGENCY] GBV data Focal Point/Liaison will share the data along with the following relevant caveats in writing:

1. **The data is only from *reported cases*.** The consolidated data is in no way representative of the total incidence or prevalence of GBV in any one location or group of locations. Sufficient explanation of limitations on reported cases and trends in reporting should be properly highlighted in any external communication after permission is received from contributing agencies. This information is confidential and cannot be reproduced without the authorization of the GBV administrative data actors.
2. The aggregate data is based on **non-identifiable data** submitted from GBV data partners for the purposes of:
    - GBV prevention and response program planning, monitoring and evaluation by [CONSOLIDATING AGENCY] and partners
    - Identification of programming and service delivery gaps
    - Prioritization of actions and next steps
    - Improved service delivery
    - Policy and advocacy
    - Resource mobilization
3. The data shared should be accompanied by the following **caveat:**

    The data shared is only from reported cases and is in no way representative of the total incidence or prevalence of Gender-Based violence (GBV) in [AREA OF COVERAGE]. These statistical trends are generated exclusively by GBV service providers who use the GBV administrative data system for data collection in the implementation of GBV response activities in a limited number of locations across [AREA OF COVERAGE]and with the consent of survivors. This data should not be used for direct follow-

up with survivors or organizations for additional case follow-up. The following information should not be shared outside your organization/agency. Failure to comply with the above will result in the suspension of sharing GBV statistics in the future.

Media and External Advocacy Institutions

Due to the impact it can have if data is shared inappropriately, all information requests from the media and external advocacy institutions will be carefully scrutinized. Any request for GBV consolidated statistics needs to be made in writing including information on how the data will be used to **[CONSOLIDATING AGENCY]** who can then share the information after receiving authorization from all data gathering organizations as outlined above.

By this information sharing protocol, the ISP signatories understand that they can refer any request for GBV consolidated statistics to **[CONSOLIDATING AGENCY]** who can then share the data after receiving authorization from all data gathering organizations in response to the written request. Any denial of authorization should be accompanied with an explanation that can be shared in a non-identifiable format with the requesting party at **[CONSOLIDATING AGENCY]**'s discretion.

TIME LIMIT

Once agreed, this information sharing protocol will take effect from the agreed upon date for information sharing to begin and will be on trial basis for **XX** months from the date the ISP has been signed. After this time, the signatories will review the effectiveness of, use of, and adherence to the protocol. In the absence of a new agreement, this protocol will automatically be renewed for [period of time], until a revised version[3] can be agreed upon.

To ensure regular review, an on-going agenda point on the GBV administrative data system will be included at the end of the monthly GBV coordination meetings to inform participating actors of information sharing protocol issues that require a follow-up discussion.

BREACHES

In cases of breach by any of those participating in this information sharing protocol, a meeting will be convened including all participating agencies' GBV data focal points within one week to discuss the matter and to determine appropriate action to be taken. If a meeting cannot be convened within one week or a resolution cannot be reached, then the following process should be undertaken:

- A meeting will be convened including **[OPERATIONAL LEVEL]** Senior Management Team from all participating agencies to discuss the matter and to determine appropriate action to be taken within one (1) week.
- If unresolved, the matter should be referred to the **[NATIONAL LEVEL]** within two (2) weeks of the breach or suspected breach.
- If unresolved, the matter would be referred to the GBV data Steering Committee for support within one (1) month.

This resolution process should not impact regular information sharing if resolved.

Data gathering organizations reserve the right to stop sharing data if the ISP is breached and will inform **[CONSOLIDATING AGENCY]** in writing with the reasons for stopping the flow of data. While the matter is being

[3] If it is agreed that a revision is not necessary, the dates can be updated and the agreement again signed.

resolved, and if **[CONSOLIDATING AGENCY]** is not involved, it is recommended that data gathering organizations continue to share data with **[CONSOLIDATING AGENCY]** to inform field level activities (i.e. programming and service delivery gaps). The GBV administrative data consolidated information will not be shared externally until the breach is resolved.

The resolution of a breach or suspected breach must be agreed to by all organizations who are signatories to this protocol. In the event that the resolution cannot be agreed upon, signatories have the option to terminate, in writing[4], their inclusion in the protocol and the protocol will be revised accordingly.

[4] The individual who signed the information sharing protocol would communicate the organization's withdrawal.

ANNEXES

Annex XX: Data to be shared with Consolidating Agency

Annex XX: GBV Data Focal Point Document

Annex XX: Roles and Responsibilities

Annex XX: Report to be generated and shared by Consolidating Agency with Data Gathering Organizations

Annex XX: Data Protection Protocol

Annex XX: Agreed Upon Report to Be Shared with External Actors

Annex XX: External Information Request Format

Annex XX: Contingency Plan (Optional)